Sky Bug Bounty Program Rulebook

Introduction

The Sky Bug Bounty Program (the "Program") is a program designed to preemptively detect and eliminate information security deficiencies ("Vulnerabilities") caused by program failures or design errors contained in the products, services, and websites offered by Sky Co., Ltd. ("Sky" or "we"). As a reward for their assistance with quality improvement, we will pay incentives to those who report to us (the "Reporter") information on the Vulnerabilities of products, services, and websites covered by the Program that they discover or identify (the "Vulnerability Information") in accordance with the Program. Under the Program, our Sky-SIRT (Security Incident Response Team in charge of the Program in Sky; the same hereinafter) works with several divisions of Sky to address the Vulnerabilities. In the event that any inconsistencies exist between the contents of this Rulebook and the Sky Bug Bounty Program Terms and Conditions ("Terms and Conditions"; this Rulebook and the Terms and Conditions collectively the “Terms and Conditions, etc.”), the Terms and Conditions shall prevail.

1. Products, services, and websites subject to verification

Please refer to the website regarding the Program (https://www.skygroup.jp/security-info/bugbounty/) for the list of products, services, and websites subject to verification under the Program ("Target Products"). For details on each product, service, or website, please refer to their respective websites.

2. Reporting Regulations

Rewards can be earned by those who have reported Vulnerabilities in accordance with the Program and satisfied the following conditions.

- The Reporter, the Reporter’s relatives (spouse, children, parents, or siblings), or a member of the same household as the Reporter is not an employee of Sky at the time of reporting, and has not been an employee of Sky at any time within six (6) months prior to the date of reporting (except that if multiple reports on the same or similar Vulnerability are submitted, such period should be six (6) months prior to the date of the Reporter’s first related report);
- The Reporter is not engaged in Sky’s business at the time of reporting, and has not been engaged in Sky’s business at any time within six (6) months prior to the date of reporting (except that if multiple reports on the same or similar Vulnerability are submitted, such period should be six (6) months prior to the date of the Reporter’s first related report) under consignment contracts, dispatch contracts, secondment agreements, etc.;

- The Reporter has never been engaged in product development or cloud service operations at Sky in the past;
- The Reporter can communicate with Sky-SIRT in Japanese or English; and
- The Reporter is eligible to participate in accordance with the conditions set forth in the Terms and Conditions and agrees to the Terms and Conditions.

Please refer to the following website for information on the Terms and Conditions.
https://www.skygroup.jp/security-info/bugbounty/

3. Contacting Sky about Vulnerabilities

3.1 Communication method

A Vulnerability report under the Program must be submitted through the Program Form on the website regarding the Program. Inquiries should be sent via the Inquiry Form on the website regarding the Program.

Program Form: https://www.skygroup.jp/security-info/bugbounty/entry.html
Inquiry Form: https://www.skygroup.jp/security-info/inquiry/

3.2 Reception hours

We accept submissions via the Program Form or Inquiry Form 24 hours a day, 365 days a year.

In principle, we will send a receipt confirmation within three (3) business days after your submission via the Program Form or Inquiry Form.

However, please note that it may take longer for us to respond during holiday periods such as the New Year's holiday.

4. Selection of Vulnerability Reporting Destinations

In 2004, an "Information Security Early Warning Partnership" was created in Japan with the goal of linking public and private sectors in order to facilitate smooth distribution of information and countermeasures related to Vulnerabilities of software products and web applications. At the same time, the "Information Security Early Warning Partnership Guideline" (latest version: May 2019), which was formulated based on a notice by the Ministry of Economy, Trade and Industry, were published. In accordance with those guidelines, in the event that a Vulnerability in software products or web applications is discovered, the related Vulnerability Information should be reported to the Information-technology Promotion Agency (IPA).

When a Reporter finds a Vulnerability in a Target Product, the final decision on whether to submit such information to both the IPA and Sky, or to only one of them, and if only one, whether to submit it to the IPA or to Sky, will be left to the Reporter. However, we request that the Reporter report Vulnerabilities directly to Sky through the "Program Form" mentioned in 3.1 above, even if the Reporter decides to submit the information to the IPA, so that we may begin addressing such Vulnerabilities as promptly as possible. Additionally, if you report directly to us, Sky will be responsible for reporting the Vulnerability Information to the IPA. Please note that this program aims for the early detection and remediation of vulnerabilities, and as stated in Rulebook 8.3.1, no reward will be granted for reporting a Vulnerability that Sky is already aware of. Furthermore, if the Reporter submits the information to the IPA first and then reports to Sky, and the timing of the Reporter's submission to Sky is after Sky has been notified of the Vulnerability Information by the IPA or by the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) based on the Reporter's submission to the IPA, it will be considered as reporting a Vulnerability that Sky is already aware of.

5. Handling and Disclosure of Vulnerability Information of Target Products

Sky shall handle Vulnerability Information in accordance with Sky's "Publication Process of Vulnerability Information for our Products and Services", which specifies how to handle and disclose Vulnerabilities when they are discovered in the Target Products. For details, please refer to the following website.
https://www.skygroup.jp/security-info/notice/170404.html

6. Vulnerability Reporting Process

6.1 Response process

When evaluating and responding to Vulnerability Information reported by a Reporter, Sky-SIRT shall perform the following actions:

1. Receive reports in the order they are registered via the Program Form, assign a reception number to each such report, and contact the Reporter.
2. Determine whether the Vulnerability Information falls under a Vulnerability in relation to the Target Products, and, if so, calculate the Reward amount.
3. Inform the Reporter of the evaluation results and the Reward amount.
   - A report is deemed as providing Vulnerability Information only when Sky determines that a Vulnerability exists based on the behavior of the Target Product.
   - If a report is deemed as providing Vulnerability Information, Sky will inform the Reporter of such determination and the corresponding Reward amount.

- If a report is not deemed as providing Vulnerability Information, Sky will inform the Reporter of such determination.
- If Sky determines that additional information is needed, Sky will request such additional information from the Reporter.
- Evaluation results and Reward amounts may fluctuate until the completion of the reporting process.

4. The reporting process is completed when Sky has received all of the Vulnerability Information resulting from a Reporter's investigation of a certain Vulnerability, and notifies the Reporter of its receipt.
   - Reward amounts are determined when the reporting process is completed and will not be changed thereafter, except that in the event that the Reporter violates the Terms and Conditions, etc., measures such as the withdrawal of Sky's decision to pay a Reward or a request to reimburse an already-paid Reward may be taken.
   - If the Reporter does not reply to Sky-SIRT by the due date stated in its notification of payment procedures and Reward amount, the reporting process will be deemed completed when the due date has passed, and the Reward will not be paid.

6.2 Order of Acceptance

Vulnerability reports are received in the order in which they are submitted via the Program Form, and a reception number is assigned to each submission accordingly.

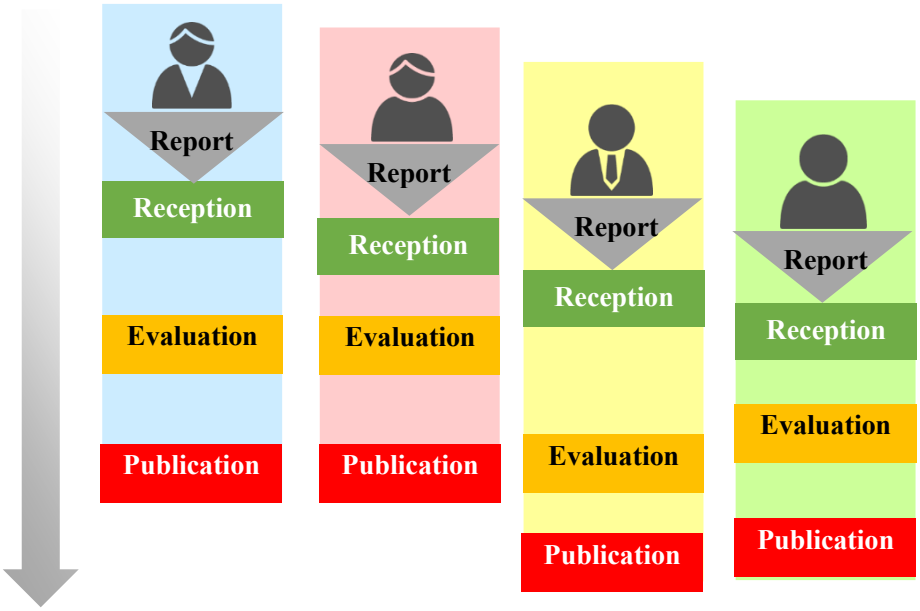
6.3 Receipt Confirmation

In principle, we will send a receipt confirmation within three (3) business days after your submission of a Program Form or Inquiry Form.

If Sky has not contacted you after seven (7) business days have passed since your submission of a Program Form, please resubmit your report via the Program Form with a note explaining the situation.

6.4 Order of Evaluation

In principle, evaluations of reports are carried out in the order of the reception number, except that the order may change depending on a report's contents. The evaluation order and the Reward amount may fluctuate until the completion of the reporting process.



7. Publication of Vulnerability Information by Reporters

If a Reporter wishes to publish, disclose, or provide any Vulnerability Information of Target Products, or any information regarding the operation that may come to his/her knowledge in the course of conducting verification investigations (including the name(s) of the Target Product(s) in which the Vulnerability was discovered; "Vulnerability Information, etc."), the Reporter shall follow the rules below.

7.1 Rules on Publication, etc. of Vulnerability Information, etc.

Please refer to the Terms and Conditions for additional information on the publication, disclosure, or provision ("Publication, etc.") of Vulnerability Information, etc.

Article 6 of the Terms and Conditions: Publication, etc. of Vulnerability Information by the Reporter
https://www.skygroup.jp/security-info/assets/docs/term.pdf

7.2 Contents and Method of Publication, etc. of Vulnerability Information, etc.

Reporters may publish, disclose, or provide Vulnerability Information, etc. only with Sky's prior consent. If you wish to publish, disclose, or provide Vulnerability Information, etc., please contact Sky via the email address used for exchanges after the submission of Vulnerability Information.

The following rules shall apply even in the event that Publication, etc. is permitted by Sky.

- Sky may adjust the contents of the Publication, etc. requested by the Reporter. If Sky approves the adjusted

contents, only the adjusted content is permitted to be published, disclosed, or provided.

- Publication, etc. is not permitted until Sky releases a modified program.
- Even after the release of the modified program, the contents that may be published, disclosed, or provided shall be limited to the fact that the Reporter has discovered a Vulnerability (i.e. the contents of Vulnerability Information, etc. may not be published, disclosed, or provided), until Sky has determined that its customers have sufficiently installed the modified program .

  Example: “I discovered a Vulnerability in Sky’s products on dd/mm/yy.”

- Sky will inform the Reporter if Sky determines that its customers have sufficiently installed the modified program. In the event the Reporter wishes to publish, disclose, or provide Vulnerability Information, etc. before receiving such notification, the Reporter shall submit a request to Sky indicating the reason therefor, and Sky may, at its discretion, specially approve such Publication, etc. prior to having issued such notification.
- In regard to Publication, etc. after Sky has determined that its customers have sufficiently installed the modified program, in principle, there are no particular restrictions on the contents of the Publication, etc., although prior approval by Sky is still required.

7.3 Modification of Target Products

Sky is continually seeking ways to improve the security of its products and services, but depending on the severity of the Vulnerability and the scope of impact of the modifications necessary to address such Vulnerability, such modifications may be delayed.

We are unable to respond to requests to expedite the implementation of modifications to address a Vulnerability for the purpose of disclosing Vulnerability Information, etc.

8. Rewards

Under the Program, Reward amounts are calculated using CVSS scores as the base score. An amount corresponding to the importance of the Vulnerability Information is added to the base score, and the sum of these amounts is the Reward amount.

CVSS scores are based on the Common Vulnerability Scoring System (CVSS), and are evaluated by the IPA, but it will take some time before the CVSS scores are finalized and published by JVN (Japan Vulnerability Notes).

If requested to do so by the Reporter, Sky may calculate the CVSS scores on its own using the CVSS and pay the Reward. However, in this case, even if the value calculated by Sky is different from the value published by JVN after such payment has been made, Sky will not make any additional compensation or issue a request for a refund of the Reward. If JVN publishes the CVSS scores during the reporting process, the Reward shall be calculated using the published scores.

8.1 Basic rule

In principle, Reward amounts are calculated using the following formula, with CVSS v3 Base Scores as the principal factor.

Reward amount = ([Basis Amount as set forth in 8.2.1] + [Additional Amount as set forth in 8.2.2]) × [Ratio as set forth in 8.2.3]

However, if there are any other factors to consider other than those mentioned in 8.2.1, 8.2.2, and 8.2.3, Sky may adjust the Reward amount at its discretion.

8.2.1 Basis amounts

In calculating Reward amounts, a Basis Amount grounded on the CVSS v3 Base Score is determined in accordance with the following tables.

Please refer to the "Overview of Common Vulnerability Assessment System CVSS v3" published by the IPA for information on CVSS v3 Base Scores.
https://www.ipa.go.jp/security/vuln/CVSSv3.html

Severity	CVSS v3 Base Score	Basis Amount
Urgent (Critical)	9.0 - 10.0	CVSS v3 Base Score × 50,000 JPY
Important (High)	7.0 - 8.9	CVSS v3 Base Score × 30,000 JPY
Warning (Medium)	4.0 - 6.9	CVSS v3 Base Score × 10,000 JPY
Note (low)	0.1 - 3.9	
None	0	No Reward

8.2.2 Additional amounts

An additional amount in consideration of the importance of the Vulnerability Information is determined according to the following classifications.

We recognize that if Reward amounts are determined solely on the basis of the CVSS score, the degree of impact on our customers using our products/services and such Reward amounts may not necessarily be commensurate. Accordingly, when calculating Reward amounts under the Program, we link the degree of impact on our customers and Reward amounts. For Vulnerabilities that fall under any of the following categories, the amount specified for each category is added to the Basis Amount. However, the total of the Basis Amount and the Additional Amount

shall not exceed 2 million JPY per Vulnerability.

Classification	Category	Additional Amount (Maximum)
RCE※ Evaluation	RCE	1,500,000 JPY
	Other than RCE	500,000 JPY
Vulnerability Category	SQL injection	250,000 JPY
	Injection (other than SQL injection)	100,000 JPY
	Defect in access control	300,000 JPY
	Defect in input confirmation	250,000 JPY
	XSS	70,000 JPY
	Others (Depending on the contents of the report, Sky may create a new category. The amount set out in the right-hand column is the maximum amount in the case of a report not falling under any of the categories listed above, and the additional amount shall be evaluated and determined in accordance with the newly created category.)	300,000 JPY

※ Arbitrary commands or codes may be executed remotely.

8.2.3 Impact of Vulnerabilities on Customers and the Ratio to the Maximum Amount for each category

Furthermore, based on the degree of impact on our customers by the reported Vulnerabilities, we will calculate the ratio by which the sum of 8.2.1 and 8.2.2 above (maximum value) will be multiplied in accordance with the following classifications.

1. Products and Cloud Services

Level of Impact of the Vulnerability Information on Sky's Customers	Ratio to the maximum value
Damage to customers caused by the Vulnerability already has been detected, and Sky has created and released or will create and release a program on an urgent basis to correct the problem	100%
Attacks on customers caused by the Vulnerability already have been detected, but no damage to customers has occurred, and Sky has created and released or will create and release a program to correct the problem	75%

No attacks on customers caused by the Vulnerability have been detected, but Sky has created and released or will create and release a program to correct the problem	50%
No attacks on customers caused by the Vulnerability have been detected, and the problem may be handled temporarily by a workaround which does not involve Sky's provision of a program to correct the problem	25%
No attacks on customers caused by the Vulnerability have been detected, and the problem may be addressed during the course of ordinary version upgrades	25%
The Vulnerability exists with respect to a part that was not developed by Sky, and, as a result of investigation, was found to be caused by another company's module, etc. which Sky uses	0%

2. Websites Published by Sky

Level of Impact of the Vulnerability Information on Sky's Customers	Ratio to the Maximum Amount
Damages such as the leakage of personal information of users of the website already has occurred, and Sky has taken or will take urgent actions to address this issue, such as shutting down or upgrading the website or posting notices to the users of the website	100%
Damage such as the leakage of information other than personal information of users of the website already has occurred, and Sky has taken or will take urgent actions to address this issue, such as shutting down or upgrading the website or posting notices to the users of the website	50%
Manipulation of the website has been detected or will be detected, but was recovered by restoration	20%
No damage to the website has been detected or will be detected, and the website was normalized by upgrading	15%

Since there is no Basis Amount grounded on the CVSS score for websites, the Reward amount generally will be the amount obtained by multiplying the Additional Amount in Appended Table 2 by the ratio above.

8.3.1 Supplementary Information on Earning Rewards

The following is supplementary information on Vulnerability Information:

1. When multiple Vulnerabilities are detected by Sky's investigation
   If Sky conducts an investigation based on a Vulnerability Information and discovers Vulnerabilities that are distinct from the reported Vulnerabilities, the Reporter shall be eligible to receive a Reward based on the Vulnerabilities reported by the Reporter, but not for any additional Vulnerabilities detected by subsequent investigations by Sky.
2. When Vulnerabilities resulting from the same cause are reported
   If Vulnerability Information for the same product, service, or website resulting from the same cause are reported, we will only certify the Vulnerability Information which was submitted first (i.e., the report which

has the earliest reception number), and a Reward shall only be issued to the Reporter of the certified Vulnerability Information.

3. When a known Vulnerability is reported
   If a Vulnerability already known to Sky is reported, no Rewards shall be issued.
4. When a Vulnerability which exists in an environment for which Sky does not guarantee operations is reported
   Rewards cannot be issued if Vulnerability Information is reported outside of an environment for which Sky guarantees operations. For details on operation guarantees, please refer to the respective websites of each product or service.
5. When Vulnerability Information on third party products used within a product, service, or website is reported
   Vulnerabilities of products other than those developed by Sky can be verified only with respect to the Vulnerabilities of which Sky is not aware, and for these products, the Reward amount which can be earned shall be calculated by the CVSS values stipulated in 8.2.1 (Base Amount) multiplied by the ratio stipulated in 8.2.3 (which differ depending on the products/cloud services and websites released by Sky).
6. When Vulnerabilities in third-party modules that we use are reported, they shall be subject to the Program if it is necessary for us to take action after having found such Vulnerabilities in our products, services, or websites. However, this shall not apply in cases where a Vulnerability is found to be caused by the module, and not by parts that are developed by us. Additionally, even if the support period defined by the provider of the module has ended, the Program may still apply.
   However, the following Vulnerabilities are not included in the Program.
   - Problems caused by web browser resources
   - Denial of Service (DoS) attacks that generate a large amount of data/requests
   - Vulnerabilities resulting from man-in-the-middle attacks

8.3.2 Criteria of Vulnerabilities resulting from the same cause

Examples of Vulnerabilities determined to result from the same cause include, but are not limited to the following. If Vulnerabilities are determined to have resulted from the same cause, Section 2 of 8.3.1 above will apply.

- When a Vulnerability is revealed in both parameters and hashes
- When websites running on the same server are affected by Vulnerabilities resulting from configuration settings
- When Vulnerabilities exist in multiple locations within the same product, service, or website due to the use of the same logic or function, etc.

Vulnerabilities resulting from the same cause are considered to constitute a different Vulnerability when the affected products, services, and websites are different. However, when the functionality of the cloud version of a product in which a Vulnerability is discovered is implemented in the packaged version, and Vulnerabilities resulting from the same cause occur in the packaged version, the Vulnerability Information is not considered to be specific to the cloud version.

8.3.3 Criteria for Similar Vulnerabilities

Examples of similar Vulnerabilities are, but not limited to, the following. If Vulnerabilities are determined to be similar, Section 2 of 8.3.1 above will apply.

- When multiple different Vulnerabilities occur due to the distribution of similar logic within the same product, service, or website

Similar Vulnerabilities are considered to be different when the affected products, services, and websites are different. However, when the functionality of the cloud version of a product in which a Vulnerability is discovered is implemented in the packaged version, and similar Vulnerabilities occur in the packaged version, the Vulnerability Information is not considered to be specific to the cloud version.

8.4 Delivery of Rewards

In principle, Rewards shall be paid by wire transfer by the end of the second month following the date of completion of the reporting process of the Vulnerability Information reported by the Reporter.

The Reporter is required to notify Sky of his/her bank account information. If the Reporter does not contact us with his/her bank account information, we may not be able to execute the payment. The same applies to cases in which the Reporter is unable to receive Rewards, even though the remittance procedures were performed in accordance with the bank account information provided by the Reporter.

8.5 Taxes

Please note the following in regard to tax liability related to the Rewards.

- A Reporter may be obliged to file an income tax return on his/her own if the amount of Rewards earned by the Reporter exceeds a certain amount. Reporters are responsible for confirming their own tax liability in relation to Rewards.
- Depending on the location of the Reporter, he/she may be required to pay taxes outside Japan. Reporters are responsible for confirming their own tax liability related to Rewards.
- Sky will not provide any support with respect to the tax liability of Reporters in relation to Rewards.

9. Free Rental of Verification Environments

Verification environments will be provided to the Reporters free of charge when a Reporter who is unable to use the necessary environment(s) to conduct additional investigations on the Vulnerability he/she has found submits a request for such a verification environment and Sky approves such request, limited to the time period that we approve. If

you wish to utilize verification environments in the manner described above, please contact us via the Program Form.

In addition, given that most of our products and services are targeted at corporate customers, and that Reporters are often unable to verify websites in the relevant environments, we will provide access to verification environments free of charge from time to time to those who have not yet submitted any Vulnerability reports. If you have difficulty in obtaining the Target Products or in carrying out verifications on websites, please access the website regarding the Program, on which we recruit applicants. If there are too many applications, Sky will select certain applicants at its discretion, and contact those who are selected.

10. Acknowledgements

We are grateful for your assistance with improving the quality of our products, services, and websites. We will post the names of Reporters who discover and report Vulnerabilities in accordance with the Program on the following website (if you do not wish to be listed, you will not be listed). Please indicate whether you wish to be listed and the name you wish to use (identity name for publication) in the Program Form.
<Those who have assisted with improving quality>
https://www.skygroup.jp/security-info/thanks/

11. Amendment of this Rulebook, etc.

Sky may amend this Rulebook, etc. without prior announcement.

In the event that Sky intends to amend the Rulebook, etc., Sky shall determine the effective date of such amendment and, prior to such effective date, post and publicize the contents of the modified Rulebook, etc., together with its effective date, on the website regarding the Program.

If a Reporter Participates in the Program on or after the effective date of the amendment based on the preceding paragraph, or has Participated in the Program prior to the effective date of the amendment and continues to Participate after the said date, the Reporter shall be deemed to have consented to the contents of the amended Terms and Conditions.

The Japanese version of this Rulebook, etc. shall constitute the official version, and the Japanese version shall prevail over any translations in other languages with respect to any interpretation thereof.

Updates
First Edition: March 2nd, 2022